BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

34

D14

PROJECT MobIDIC

Systems Analysis

Version 1-2 17-01-97

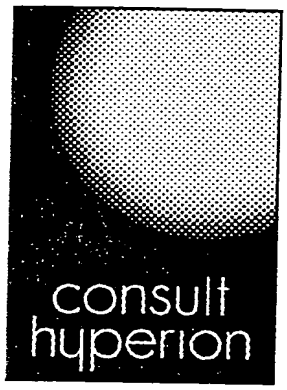


TABLE of CONTENTS

1. Introduction

1.1 Overview

Project MobIDIC has been set up to investigate and, if commercially viable, launch information services to support mobile customers (as workers and consumers) who carry a Personal Digital Assistant (PDA). These services must support delivery and transmission of information from the PDA using an "air interface" (specifically via GSM networks) and typically will be provided using Internet protocols. Support for existing Internet services, primarily World Wide Web browsing must be offered.

MobIDIC is investigating (by prototyping and piloting) the feasibility of a 'softgoods' electronic commerce service and opportunities for mobile Internet based data services. The team are using smart cards and electronic cash for the payment mechanisms and identification. The cards will be connected to small portable computers running an internet browser connected to the Internet via a GSM data service. Example services will be available to demonstrate three principal payment types:

- consumer to retailer, to pay for:
    - database query
    - file download[1]
    - time behind a link[2]
- bank to consumer
    - electronic cash withdrawal
    - electronic cash deposit
- consumer to consumer

In the 'softgoods' e-commerce business plan, there are two principal markets envisaged: private networks (intranet) and public networks (Internet). The commerce concepts are network and access device independent. Mobile access devices were selected as the target clients because of the easy and

[1] Not available at pilot launch

[2] Not available at pilot launch

low cost way in which network access can be offered and because of the importance of mobile access to the European market.

The Mobile data opportunities also divide similarly into two segments: private networks and public networks. The private networks further subdivide into 'Blue Collar' and 'White Collar' workforces.

1.2 Purpose and Scope

The main purposes of this document are, given the business requirements documented in (BA), to:

- list the "events" through which the system as a whole will be stimulated to provide some response
- describe the "user view" of each event
- present a high level system architecture
- with reference to the system architecture, specify the underlying processing and messaging caused by each event, with particular emphasis on interfaces where components are to be developed by different parties.

Detailed interface specifications, which are necessary to ensure that systems produced by different organisations will work together to produce the intended results will be produced later, derived from this document.

From the interface specifications, software specifications will be produced for components requiring a high level of bespoke software development.

1.3 Related Documents

(BA) MobIDIC Business Analysis, Version 3.0, 08Oct96

(IFD-IFD) Mondex IFD-IFD Application Interface Specification, Version 2.0, 17Nov95

(IFD-PA) Mondex IFD Purse Application Interface Specification, Version 1.0, 17Nov95

1.4 Structure

The remainder of this document has the following structure:

2. EXTERNAL EVENTS, specifying the external events
3. USER INTERFACE, giving a high level description of the "user experience"

4. ARCHITECTURE, describing the main components

5. INTERFACES, specifying message flows between components.

2. External Events

External events cause the system as a whole, to take some action which may be:

(1) to output some information

(2) to change the system's state, i.e. to alter its response to some future external event

(3) a combination of (1) and (2).

The events are classified in the table below according to whether they are issued by "end users" from PDAs (prefixed by 'U') by systems administrators (prefixed by 'A') or by electronic links to external systems (prefixed by 'E').

Note that many of the requirements in (BA) are not directly represented below because the requirements are fulfilled as a consequence of one of the events: thus Requirement R10 "Clients shall be able to pay for items delivered by http using an electronic purse" is met as a consequence of the processing initiated by Events U1, U2 and U3.

Event	Description
U1	Request restaurant search
U2	Request event search
U3	Request flight information
U4	Request GIN information For the initial phase of the pilot only 'request/response' commands will be supported; 'trigger' commands will be implemented only if time allows.
U5	Withdraw Mondex cash
U6	Deposit Mondex cash
U7	View bank account balance
U8	Clear Mondex card exception log
U9	Unlock "locked out" Mondex card

A1	Initialise restaurant information This will be a one-off process at the start of the pilot; if further pilot phases are planned, a means of keeping this information current will be devised
A2	Initialise event information This will be a one-off process at the start of the pilot; if further pilot phases are planned, a means of keeping this information current will be devised
A3	Initialise flight information This will occur on a daily basis, with flights for "today" and "tomorrow" loaded.
A5	Update GIN information This utilises the existing GIN services; no new processing is required
A6	Set up bank accounts At the discretion of NatWest Bank, these could be "stand alone" accounts, with no means of access other than via the MobIDIC facilities (e.g. ATMs cannot be used)
E1	Update flight information This occurs in real time

3. User Interface

3.1 Restaurant Search

I. using the standard browser interface, the user will view Timeout's MobIDIC home page

II. the home page will present options to "search for restaurant" and "search for event"

III. on selecting "restaurant", the user will be presented with a form, with "check box" options for:
- area
- cuisine type
- payment methods
- air conditioning.

IV. on submitting the form the user will be presented with a list of restaurants satisfying the criteria (each in the form of a hypertext link), with a commentary of the form "10p to view restaurant detail"

V. on selecting a restaurant, the user will be presented with a Mondex wallet screen, stipulating the price, a reminder to insert a Mondex card and an option to pay or cancel

VI. on selecting 'pay':

A. the user is presented with a Newton "name card" containing the restaurant information, stored within the "In box"

B. a "digital receipt" containing details of the purchase (vendor, item, price) will also be filed in the "In box", but will not be automatically displayed to the user

VII. on closing or filing the name card, the user will return to the screen listing the restaurants which satisfied the search parameters, and may wish to select another restaurant or browse elsewhere.

3.2 Event Search

I. using the standard browser interface, the user will view Timeout's MobIDIC home page

II. the home page will present options to "search for restaurant" and "search for event"

III. on selecting "event", the user will be presented with a form, with "check box" options for:
- artist
- venue
- date
- price.

IV. on submitting the form the user will be presented with a list of events satisfying the criteria (each in the form of a hypertext link), with a commentary of the form "10p to view event detail"

V. on selecting an event, the user will be presented with a Mondex wallet screen, stipulating the price, a reminder to insert a Mondex card and an option to pay or cancel

VI. on selecting 'pay':

A. the user is presented with a Newton "meeting slip" containing the event information, stored within the "In box"

B. a "digital receipt" containing details of the purchase (vendor, item, price, etc.) will also be filed in the "In box", but will not be automatically displayed to the user

VII. on closing or filing the meeting slip, the user will return to the screen listing the events which satisfied the search parameters, and may wish to select another event or browse elsewhere.

3.3 Request Flight Information

I. using the standard browser interface, the user will view Schiphol's MobIDIC home page

II. the home page will present options for "arrivals" and "departures"

III. on selecting one of the above options, the user will be presented with a form to enable searching/selection based on some combination of:
- airline
- flight number
- arrival/departure time at Schiphol
- originating or destination city/airport.

IV. on submitting the form the user will be presented with a list of flights satisfying the criteria (each in the form of a hypertext link), with a commentary of the form "10p to view event detail"

V. on selecting a flight, the user will be presented with a Mondex wallet screen, describing the "goods" to be purchased, the price, a reminder to insert a Mondex card and an option to pay or cancel

VI. on selecting 'pay':

A. the user is presented with a Newton "meeting slip" containing the flight information, stored within the "In box"

B. a "digital receipt" containing details of the purchase (vendor, item, price) will also be filed in the "In box", but will not be automatically displayed to the user.

VII. on closing or filing the meeting slip, the user will return to the screen listing the flights which satisfied the search parameters, and may wish to select another flight or browse elsewhere.

3.4 Request GIN Information

1. user fires up GIN specific package on Newton
2. user selects information category from range of icons (taken from GIN brochure ware)
3. user selects specific query using pull down menus and possibly other Newton "look and feel" artefacts
4. user submits query by tapping a 'Submit' button
5. results of query, are stored in the In box and displayed to the user in a textual form
6. on closing or filing the results, the user is returned to the screen showing icons representing the categories of GIN services.

3.5 Withdraw Mondex cash

1. user accesses NatWest Bank's MobIDIC home page, which reminds him that his Mondex card must be inserted to access his account, and provides a button to tap when the card is inserted
2. assuming the correct Mondex card is inserted, the user will be presented with a screen which displays
   - account name and number
   - an account balance (note that most bank accounting systems do not provide real time balances; balances are usually updated daily)
   - funds available for withdrawal (based upon account balance and a daily limit)
   - a field for entering an amount of money (in pounds sterling) to be withdrawn (or deposited)
   - buttons for initiating a Mondex withdrawal or deposit and for accessing customer service.

3. when the user taps 'withdraw', assuming funds are available, he is displayed the same screen but with updated 'balance' and 'available' figures.

3.6 Deposit Mondex cash

1. user accesses NatWest Bank's MobIDIC home page, which reminds him that his Mondex card must be inserted to access his account, and provides a button to tap when the card is inserted.

2. assuming the correct Mondex card is inserted, the user will be presented with a screen which displays:
   - account name and number
   - an account balance (note that most bank accounting systems do not provide real time balances; balances are usually updated daily)
   - funds available for withdrawal (based upon account balance and a daily limit)
   - a field for entering an amount of money (in pounds sterling) to be deposited (or withdrawn)
   - buttons for initiating a Mondex withdrawal or deposit and for accessing customer service.

3. when the user taps 'withdraw', assuming funds are available, he is displayed the same screen but with updared 'balance' and 'available' figures.

3.7 View Bank Account Balance

1. user accesses NatWest Bank's MobIDIC home page, which reminds him that his Mondex card must be inserted to access his account, and provides a button to tap when the card is inserted

2. assuming the correct Mondex card is inserted, the user will be presented with a screen which displays:
   - account name and number
   - an account balance (note that most bank accounting systems do not provide real time balances; balances are usually updated daily)
   - funds available for withdrawal (based upon account balance and a daily limit)
   - a field for entering an amount of money (in pounds sterling) to be deposited (or withdrawn)
   - buttons for initiating a Mondex withdrawal or deposit and for accessing customer service.

3.8 Clear Mondex Card Exception Log

1. the user will be alerted by the Newton whenever a card is inserted with a full exception log and advised to contact the issuing bank's customer service.

2. user accesses NatWest Bank's MobIDIC home page, which reminds him that his Mondex card must be inserted to access his account, and provides a button to tap when the card is inserted

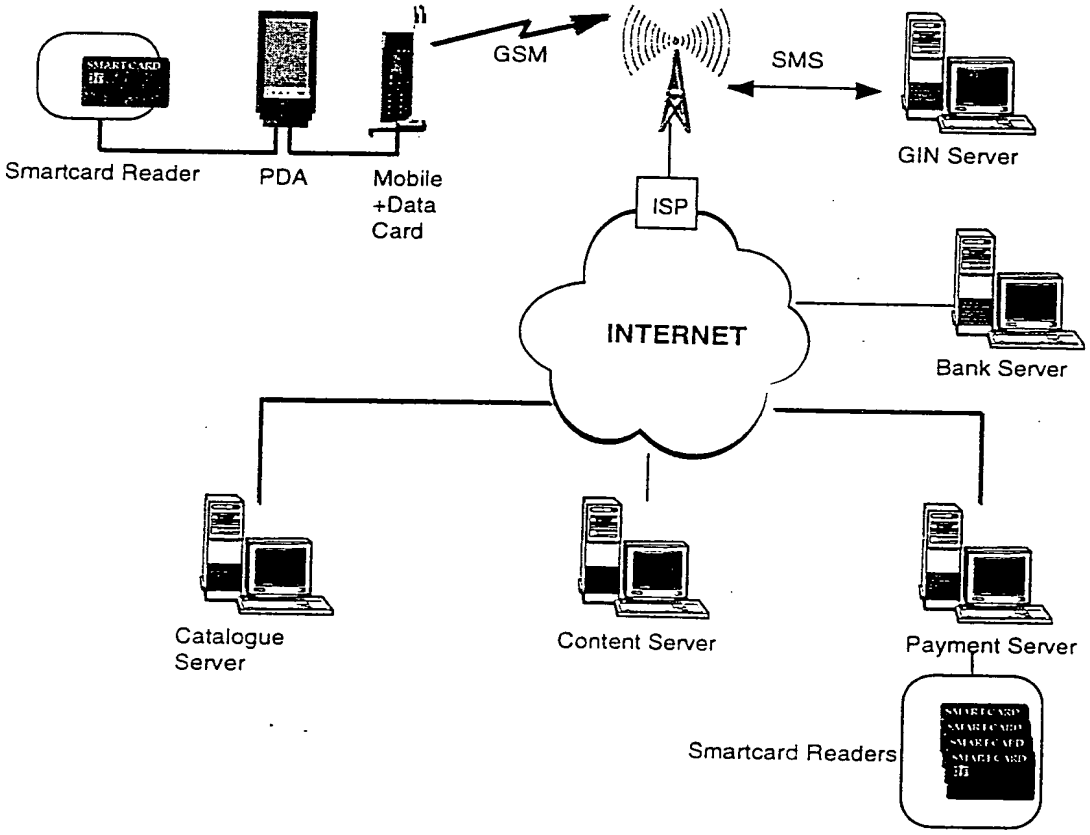
3. assuming the correct Mondex card is inserted, the user will be presented with a screen which displays
   - account name and number
   - an account balance (note that most bank accounting systems do not provide real time balances; balances are usually updated daily)
   - funds available for withdrawal (based upon account balance and a daily limit)
   - a field for entering an amount of money (in pounds sterling) to be deposited (or withdrawn)
   - buttons for initiating a Mondex withdrawal or deposit and for accessing customer service.

4. on tapping 'customer service', user is presented with a screen prompting the user to return the card to NatWest for exception log to be cleared.

4. Architecture

4.1 Logical Architecture

The following diagram shows the logical architecture, for the initial pilot and beyond, which will fulfil generalised requirements of the kind specified in (BA) by supporting the external events and end user interfaces specified in previous sections of this document.



The high-level functions of the various logical servers involved in a retail purchase need to be specified at this stage:

Logical Server	Function
Catalogue	Provides a well-organised and presented description of goods for sale, together with prices and acceptable payment methods for the client to select
Payment	Accepts payment from the client for defined goods by the selected mechanism, and returns a digital receipt
Content	Supplies digital goods to the client against a digital receipt

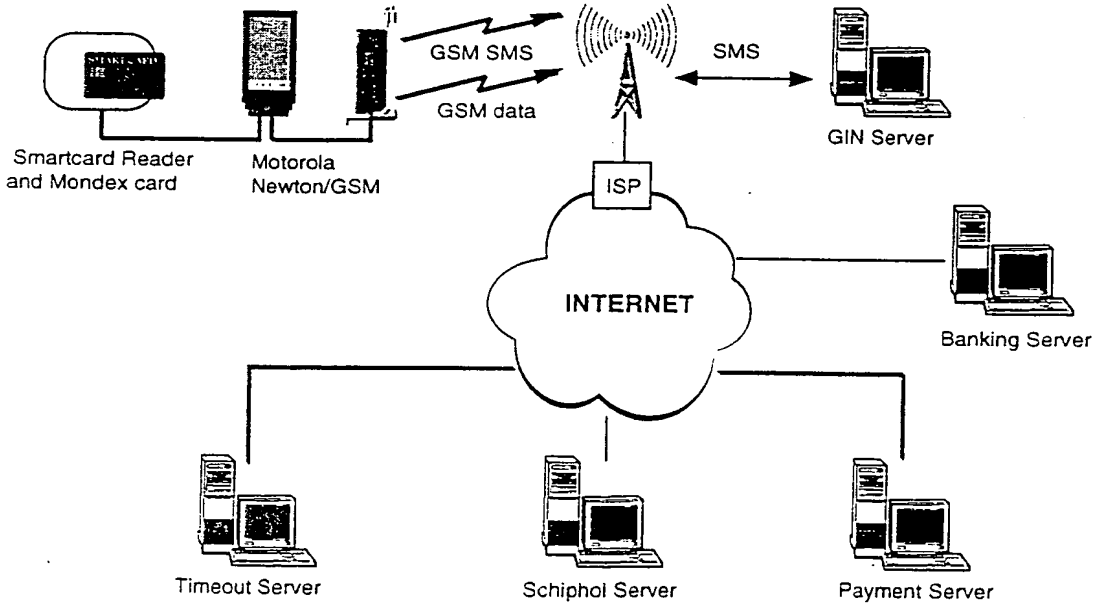
The following points need to be made regarding these logical servers:

- in a full service, the purchase of any particular item may involve the three servers operated by different organisations and in different locations
- conversely, three logical servers may be implemented in one physical server.

4.2 Physical Architecture

4.2.1 Overview

The physical architecture for the initial pilot is shown below.

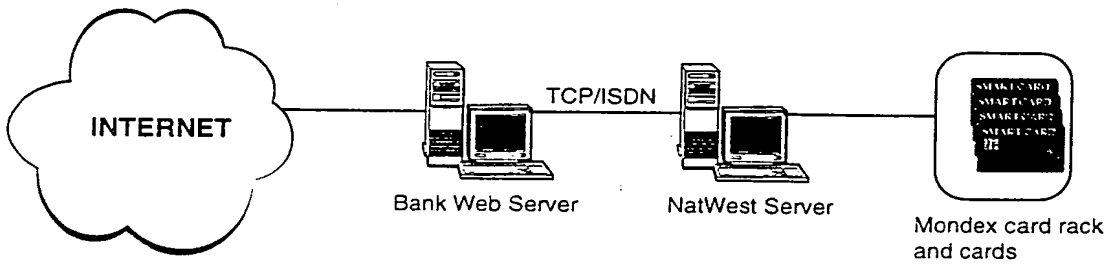


Some of the servers have some internal structure which is important from the point of view of development and operations. These structures are shown in the following sections.

4.2.2 Banking Server

The Banking server is comprised of two components, linked by an ISDN connection:

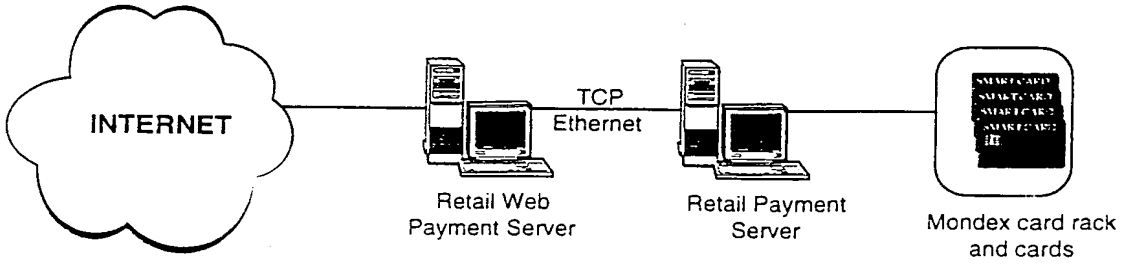
- the NatWest Server which implements the banking functions, accessible via TCP/IP connections and controls a rack of Mondex cards.
- the Bank Web Server, which presents for clients an html interface to the functions provided by the NatWest server.



4.2.3 Payment Server

The payment server is comprised of two components, linked by an ethernet LAN:

- the Retail Payment Server, which implements the payment function (i.e., receipt of Mondex value for purchases), accessible via TCP/IP connections and controls a rack of Mondex cards.
- the Retail Web Payment Server, which makes the payment function accessible over the Internet using the MobIDIC shopping protocol.

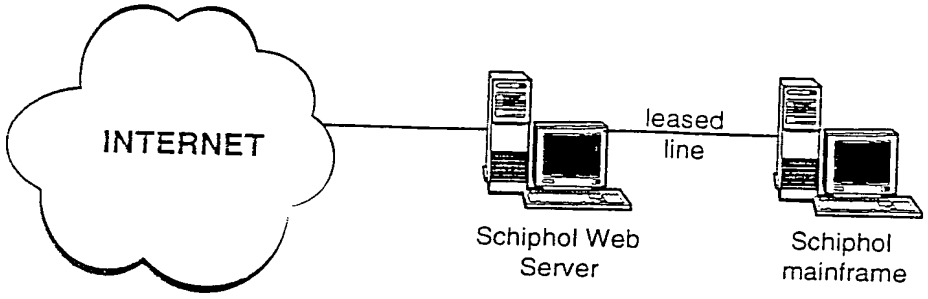


4.2.4 Schiphol Server

The Schiphol Server consists of:

- Schiphol's existing mainframe system with a new leased line interface to the Schiphol web server

- Schiphol Web Server, which maintains an image of the Schiphol mainframe database, which is made accessible via html pages.



4.2.5 Timeout Server

Updates to the Timeout database will be possible by secure, remote access using a standar web browser.

4.3 Responsibilities

The components are described below, together with the organisations responsible for delivering them for the initial pilot.

Component	Description	Responsibility
Smart card reader	Initially, Gemplus GCR400 serial device for ISO 7816 cards; later, Gemplus GPR400 PCMCIA reader/writer for ISO 7816 smart cards	Hardware: Gemplus PCMCIA driver: SRL
Mondex card	Sterling cards compatible with those issued in Swindon and Exeter	NatWest
Newton/GSM phone	A connected MP2000 and GSM phone	Hardware: Apple/Motorola Software: Lunatech/Hyperion
GSM Network	A UK GSM cellular network	Vodafone
ISP	An Internet Service Provider	Lunatech
GIN Server	The existing GIN server	GIN

Timeout server	A combined catalogue and content server, based on a Macintosh web server	Development: Hyperion Live data: Timeout Operations: Lunatech
Schiphol Web Server	A combined catalogue and content server, based on a Unix web server	Development: Lunatech Live data: Schiphol Operations: Lunatech
Schiphol mainframe	Existing mainframe information system, with extra leased line interface to Schiphol Web server	Upgrade: Schiphol Operations: Schiphol
Retail Web Payment Server	Provides a www front end to the Retail Web Server	Interface to RPS spec: NatWest Bank Interface to client spec: Hyperion Development: Unisource/SRL Operations: Lunatech
Retail Payment Server (RPS)	A Mondex- capable payment server, accessible via TCP/IP	Specification and development: NatWest Bank Operations: Lunatech
Mondex card rack	A peripheral providing a multiplicity of card readers	NatWest Bank
Bank Web server	Provides a www front end to the NatWest server (NWS)	Interface to NWS spec: NatWest Bank Interface to client spec: Hyperion Development: Unisource/SRL Operations: Lunatech

NatWest server (NWS)	A server allowing withdrawal / deposit of Mondex value versus account debit / credit	NatWest Bank

5. Interfaces

5.1 Introduction

This section specifies message flows between components which result from certain of the external events specified in Section 2. In particular, it specifies messaging related to novel functionality provided by MobIDIC, in particular payment functionality, in the following contexts:

"shopping", resulting from events U1, U2 and U3

"banking", resulting from events U5, U6 and U7.

5.2 MIME types

The shopping and banking protocols are defined in terms of a number of new MIME types. All of these MIME types have the same syntax. Specifically, they consist of a series of fields as follows:

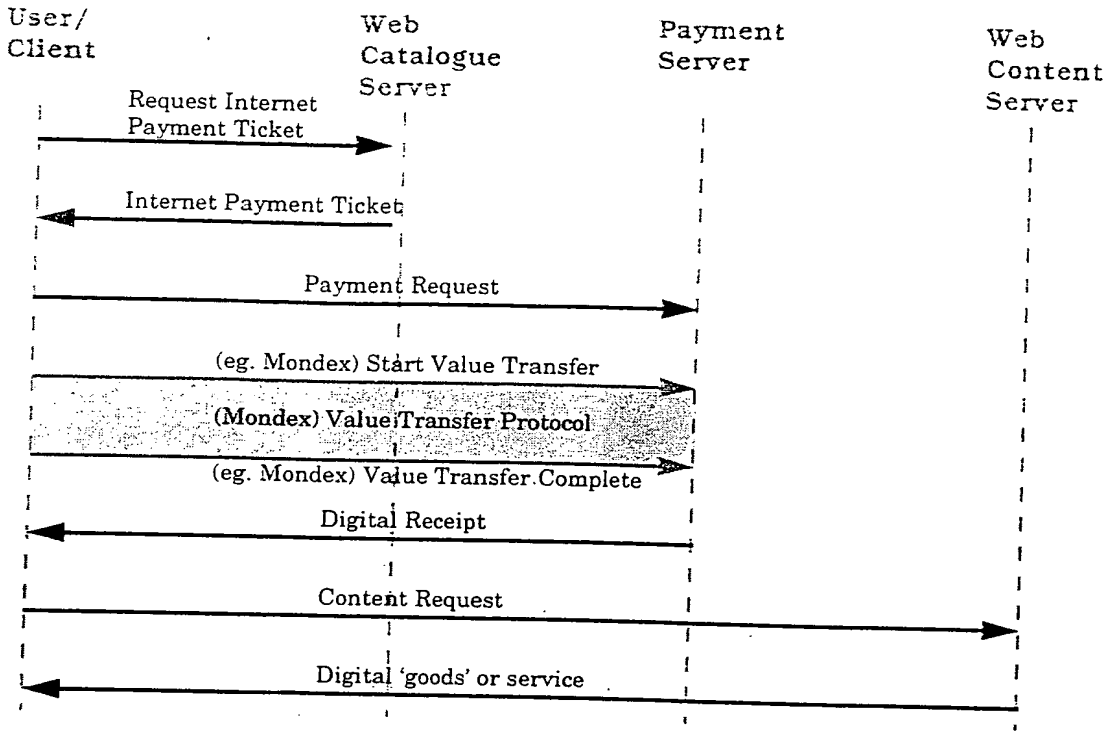
- `{<label>value}`
- where '<' and '>' are literal ASCII characters delimiting labels and values
- `label` is a variable length field identifier consisting of ASCII characters
- `value` is one of the following:
    - variable length ASCII field
    - fixed length binary field
    - variable length binary field (only permissible as the last field of a message)
- `{...}` indicates repetition (i.e. not literal characters in messages / files).

Fields may appear in any order, with the exception that a single variable length binary field, if present, must be the last field in the message.

5.3 Shopping Protocol

5.3.1 Overview

The diagram below shows an overview of the shopping protocol , in terms of the logical architecture. For the pilot, catalogue server and content server functionality will be combined (in the Schiphol server and in the Timeout server).



The initial message "Request Internet Payment Ticket" is generated by the browser when the user selects an item to buy (Stage V in the user descriptions of Events U1, U2, U3 (Section 3)). Stage V is completed with the receipt of the Internet Payment Ticket, from the Catalogue Server (Schiphol Server or Timeout Server) which triggers the launch of the payment helper (i.e. a Mondex wallet screen).

When the user confirms his acceptance of the proposed transaction (Stage VI), via the wallet screen, the helper sends an "Internet Payment Request" based upon the Internet Payment Ticket, to the Payment Server.

Based upon the selected payment method (specified in the Internet Payment Request), a payment will be initiated using the appropriate method. The only supported method for the pilot will be Mondex. The Mondex payment will be initiated by the "Start Value Transfer" message as specified in (IFD-IFD). The rest of the Mondex payment will be achieved as per (IFD-IFD), culminating in the Mondex Wallet helper sending a "Value Transfer Complete" message to the Payment Server.

On receipt of the Value Transfer Complete message (or equivalent message from a payment mechanism which may be supported in the future), the Payment Server will return a "Digital Receipt".

The digital receipt will be forwarded in a "Content Request" message to a Content Server (i.e. the Schiphol Server or the Timeout Server). The Content Server will then check the authenticity of the digital receipt and deliver the purchased information.

5.3.2 Request Internet Payment Ticket

This is a standard http request from the browser indicating the user has selected a hypertext link.

5.3.3 Internet Payment Ticket

This is an http response containing the MIME type APPLICATION/IPT. Fields defined for this MIME type for the pilot service are as follows:

label	Description	Encoding of value	Permissible values for pilot
VER	Version of this MIME type	unsigned binary value in 1 byte field	1
REF	Product reference code; must be unique within the 'CON' URL (see below)	ASCII characters	Can be assigned by developers of Schiphol and Timeout servers
PRC	Price in minor unit of currency (i.e. penny or cent, etc.)	binary value in 6 byte field, MSB first (as per (IFD-PA))	1 to 50,000 (pence)
CUR	Currency to be used in purchase	3-letter ISO 4217code	Only 'GBP' is valid
MTH	Acceptable payment methods	Concatenated 4-character ASCII sub-fields, as per ISO 7816 registration: thus 'MXPACHIP' would indicate Mondex and Chipper are acceptable methods	Only 'MXPA' valid
CAT	Unique identifier for catalogue	ASCII	Catalogue server's URL: denoting either Schiphol server or Timeout server

PAY	URL of payment server	ASCII	Only one value will reach the payment server
CON	URL of content	ASCII	Either on the Schiphol or Timeout physical server

5.3.4 Payment Request

As per Internet Payment Ticket with the exceptions:

- MIME type APPLICATION/IPT embedded within http request
- MTH must specify one method only, based on client preference. Clearly this is 'MXPA' for the pilot.

5.3.5 Mondex Value Transfer

As per (IFD-IFD); all messages are over 'raw' TCP/IP connection, i.e. not http. The TCP/IP connection is initiated by the Mondex wallet helper after the dispatch of the payment request; the server must listen on port 471 for the TCP/IP connection request. At the end of the Mondex Value Transfer (i.e. after receipt of the Value Transfer Complete reply), the Mondex wallet helper terminates the TCP/IP connection.

Mondex transaction recovery will not be implemented for the pilot.

5.3.6 Digital Receipt

This is an http response (to the payment request), containing the MIME type APPLICATION/RECEIPT. Fields defined for this MIME type for the pilot service are as follows:

label	Description	Encoding of value	Permissible values for pilot
VER	Version of this MIME type	unsigned binary value in 1 byte field	1

REF	Product reference code; must be unique within the 'CON' URL (see below)	ASCII characters	Can be assigned by developers of Schiphol and Timeout servers
PRC	Price in minor unit of currency (i.e. penny or cent, etc.)	binary value in 6 byte field, MSB first (as per (IFD-PA))	1 to 50,000 (pence)
CUR	Currency used in purchase	3-letter ISO 4217 code	Only 'GBP' is valid
MTH	Payment method used	4-character ASCII sub-fields, as per ISO 7816 registration	Only 'MXPA' valid
CAT	Unique identifier for catalogue	ASCII	Catalogue server's URL: denoting either Schiphol server or Timeout server
PAY	URL of payment server	ASCII	Only one value will reach the payment server
CON	URL of content	ASCII	Either on the Schiphol or Timeout physical server

AUT	An authorisation code generated by the payment server and checked by the content server	unsigned binary 4-byte field	Payment server will allocate a unique serial number for each digital receipt; content servers may check serial number has not been presented before[3]

5.3.7 Content Request

As per digital receipt with the exception:

- MIME type APPLICATION/RECEIPT embedded within http request.

5.3.8 Digital Goods

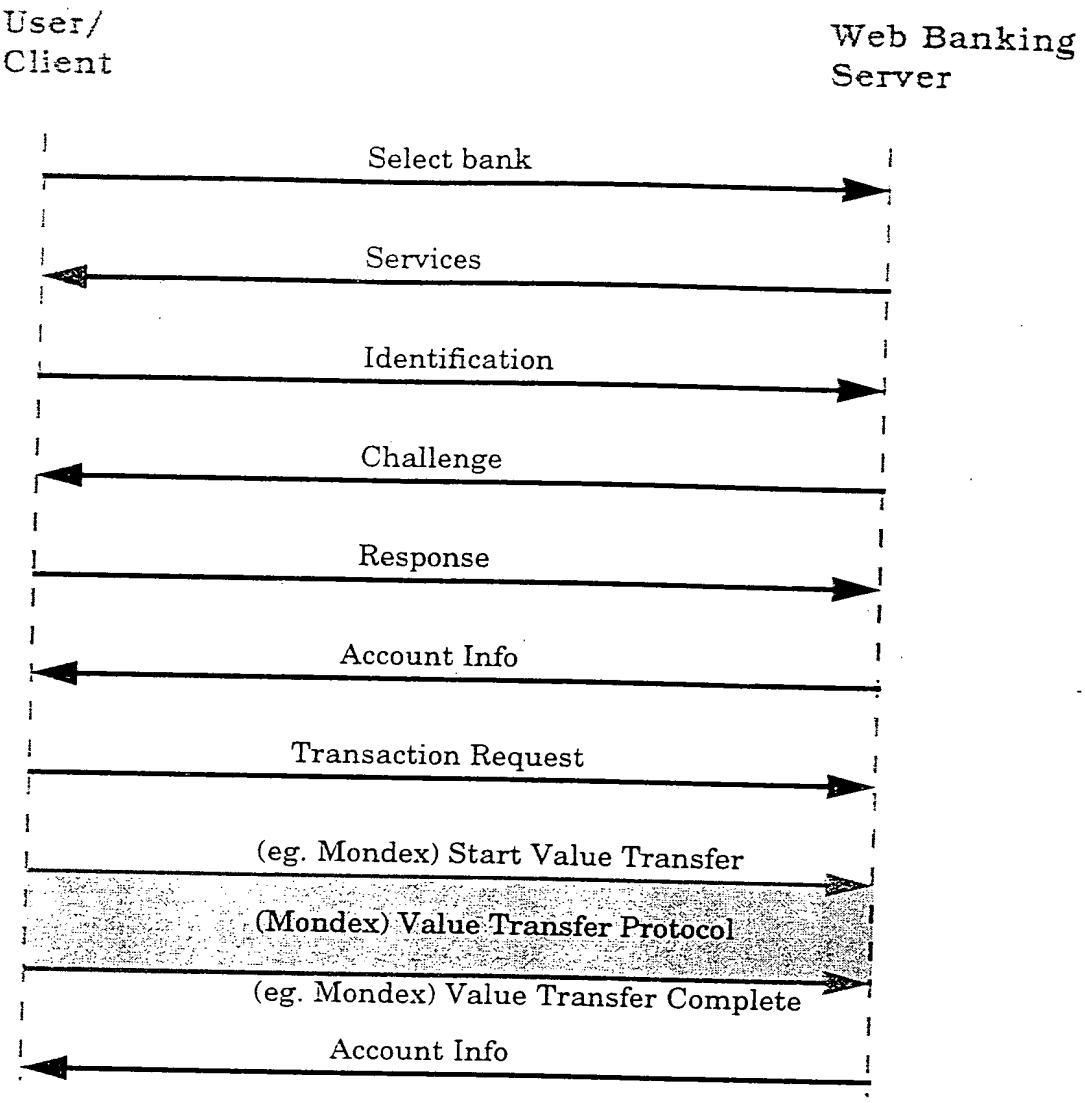
An http response.

5.4 Banking Protocol

5.4.1 Overview

The sequence of messages when the client conducts banking transactions is shown below.

[3] In the longer term, authorisation codes are likely to consist of payment server's digital signature plus public key certificate.



This scenario starts with the user viewing via the browser the MobIDIC banking home page. On selection of the "National Westminster Bank plc" hypertext link (the only one present for the pilot), the bank responds with a message indicating the services which are available. The client software then identifies the user, based on information in his smart card. The bank then issues a "Challenge" to authenticate the user. "Response" contains data for the bank to verify the presence of a legitimate user of known identity. Once this has been completed, "Account Info" is supplied to the client. On selection of "withdraw" or "deposit" an appropriate "Transaction Request" is sent to the bank followed by the initiation of a "Value Transfer" (Mondex for the pilot). On completion, an indication of a success (or failure) together with updated "Account Info" is sent to the client (for the pilot, there is no updated account information available in real time).

5.4.2 Select Bank

This is an ordinary http request initiated by selecting a hypertext link.

5.4.3 Services

This is an http response containing the MIME type APPLICATION/BANKSERV. Fields defined for this MIME type for the pilot service are as follows:

label:	Description	Encoding of value	Permissible values for pilot
VER	Version of this MIME type	unsigned binary value in 1 byte field	1
MTH	Acceptable "payment" methods	Concatenated 4-character ASCII sub-fields, as per ISO 7816 registration: thus 'MXPACHIP' would indicate Mondex and Chipper are acceptable methods	Only 'MXPA' valid
SER	Available services	Concatenated 4-character ASCII sub-fields: thus 'WITHDEPO' would indicate withdrawal and deposit services (only) are available	'WITHDEPOBALA ' indicating provision of withdrawal, deposit and account balance facilities
TAG	Session tag for Web server to link messages pertinent to the same 'run' of the client banking plug-in	4-byte binary field	Sequence number allocated by web server

5.4.4 Identification

This is an http request containing the MIME type APPLICATION/BANKID. Fields defined for this MIME type for the pilot service are as follows:

label	Description	Encoding of value	Permissible values for pilot
VER	Version of this MIME type	unsigned binary value in 1 byte field	1
SCH	Identification scheme	unsigned binary value in 1 byte field	1 = 'Mondex PID'
ID	Identification	ASCII characters	Any valid Mondex PID
TAG	Session tag for Web server to link messages pertinent to the same 'run' of the client banking plug-in	4-byte binary field	Sequence number allocated by web server

5.4.5 Challenge

This is an http response containing the MIME type APPLICATION/CHALLENGE. Fields defined for this MIME type for the pilot service are as follows:

label	Description	Encoding of value	Permissible values for pilot
VER	Version of this MIME type	unsigned binary value in 1 byte field	1
MET	Authentication method	unsigned binary value in 1 byte field	81(hex) = Mondex Personal Code Verification
DAT	Method specific data, for example random challenge	a variable number of bytes	7-byte field containing a Mondex 'random seed' (see (IFD-PA))

TAG	Session tag for Web server to link messages pertinent to the same 'run' of the client banking plug-in	4-byte binary field	Sequence number allocated by web server

5.4.6 Response

This is an http request (sic) containing the MIME type APPLICATION/RESPONSE. Fields defined for this MIME type for the pilot service are as follows:

label	Description	Encoding of value	Permissible values for pilot
VER	Version of this MIME type	unsigned binary value in 1 byte field	1
MET	Authentication method	unsigned binary value in 1 byte field	81(hex) = Mondex Personal Code Verification
DAT	Method specific data, for example response to random challenge	a variable number of bytes	Contains a Mondex 'crypto signature' (see (IFD-PA))
TAG	Session tag for Web server to link messages pertinent to the same 'run' of the client banking plug-in	4-byte binary field	Sequence number allocated by web server

5.4.7 Account Info

This is an http response containing the MIME type APPLICATION/ACCOUNT. Fields defined for this MIME type for the pilot service are as follows:

label	Description	Encoding of value	Permissible values for pilot

VER	Version of this MIME type	unsigned binary value in 1 byte field	1
BNK	Bank name	ASCII string	'National Westminster Bank'
BCH	Branch Identifier	ASCII string	An NWB sort code
NAM	Name of account	ASCII string	Not present in the pilot
ACC	Account number	ASCII string	As allocated by NWB
CUR	Currency in which account is denominated	3-letter ISO 4217 code	Only 'GBP' is valid
SER[4]	Available services	Concatenated 4-character ASCII sub-fields: thus 'WITHDEPO' would indicate withdrawal and deposit services (only) are available	expected to be 'WITHDEPOBALA' but dependent upon response from NatWest server
BAL	Account balance in minor unit of currency (i.e. penny or cent, etc.)	binary value in 6 byte field, MSB first (as per (IFD-PA))	1 to 10^6 -1 (pence)
AVL	Funds currently available for withdrawal	binary value in 6 byte field, MSB first (as per (IFD-PA))	Not present in the pilot
TAG	Session tag for Web server to link messages pertinent to the same 'run' of the client banking plug-in	4-byte binary field	Sequence number allocated by web server

[4] Optional in protocol, but to be implemented in pilot

5.4.8 Transaction Request

This is an http request containing the MIME type APPLICATION/BANKING. Fields defined for this MIME type for the pilot service are as follows:

label	Description	Encoding of value	Permissible values for pilot
VER	Version of this MIME type	unsigned binary value in 1 byte field	1
BNK	Bank name	ASCII string	'National Westminster Bank'
BCH	Branch Identifier	ASCII string	An NWB sort code
NAM	Name of account	ASCII string	Any printable characters
ACC	Account number	ASCII string	As allocated by NWB
CUR	Currency in which account is denominated	3-letter ISO 4217 code	Only 'GBP' is valid
TYP	Type of transaction	unsigned binary value in 1-byte field	0 - reserved (for no further transactions) 1 = 'withdraw' 2 = 'deposit'[5]
VAL	Value associated with transaction	binary value in 6 byte field, MSB first (as per (IFD-PA))	1 - 50,000 (pence)
TAG	Session tag for Web server to link messages pertinent to the same 'run' of the client banking plug-in	4-byte binary field	Sequence number allocated by web server

[5] Future transaction types may require additional fields.

5.4.9 Mondex Value Transfer

As per (IFD-IFD); all messages are over 'raw' TCP/IP connection, i.e. not http. The TCP/IP connection is initiated by the Mondex wallet helper after the dispatch of the transaction request; the server must listen on port 471 for the TCP/IP connection request. At the end of the Mondex Value Transfer (i.e. after receipt of the Value Transfer Complete reply), the Mondex wallet helper terminates the TCP/IP connection.

Mondex transaction recovery will not be implemented for the pilot.

Version History

Version	Date	Status
0-1	08/10/96	Pre-release for early feedback; only Sections 1-3 completed.
0-2	18/10/96	Pre-release containing component descriptions and organisational responsibilities (Section 4)
0-3	30/10/96	Pre-release containing a specification of the "shopping protocol"
0-4	05/11/96	First complete draft, including banking protocol; Minor (but crucial to implementors!) changes to shopping and banking protocols: • TCP/IP connection for value transfer initiated by client • "Value Transfer Complete" message sent by server
1-0	11/11/96	Released after review with Unisource and NatWest (6/11/96). Modifications made to banking and shopping protocols.
1-1	15/11/96	Minor modifications to user interface descriptions, reflecting the actual data available from Timeout and the existing demonstrations. Availabiltiy of remote updates to Timeout database stipulated. Responsibilities modified to reflect current project arrangements. Minor modifications to shopping and banking protocols modified following feedback from implementors. Specifically: • binary fields are in general fixed length

		• CON field added to digital receipt • SER field present in 'Account Info' message • re-defined TAG field present in all banking protocol messages • values of TYP field re-defined • monetary values are transmitted MSB first
1-2	17/11/96	Overview changed to match evolving business opportunities